BOOLEAN ALGEBRA BASED INTERDEPENDENCY MODELING FOR RELIABILITY EVALUATION OF A CYBER ENABLED POWER SYSTEM

A Thesis by

Vigneesh Murali

Bachelor of Engineering, Anna University, 2016

Submitted to the Department of Electrical Engineering and Computer Science
and the faculty of the Graduate School of
Wichita State University
in partial fulfillment of
the requirements for the degree of
Master of Science

May 2021

© Copyright 2021 by Vigneesh Murali

All Rights Reserved

BOOLEAN ALGEBRA BASED INTERDEPENDENCY MODELING FOR RELIABILITY EVALUATION OF A CYBER ENABLED POWER SYSTEM

The following faculty members have examined the final copy of this thesis for form and content and recommend that it be accepted in partial fulfillment of the requirement for the degree of Master of Science with a major in Electrical Engineering.

____
Visvakumar Aravinthan, Committee Chair

____
Ward T.Jewell, Committee Member

____
Ehsan Salari, Committee Member

DEDICATION

To all my Friends and Family

ACKNOWLEDGEMENTS

I would like to thank my advisor and mentor Dr. Visvakumar Aravinthan for giving me the opportunity to work with him and helping me throughout my masters to bring the best out of me. I sincerely thank to all my committee members and the Department of Electrical Engineering and Computer Science at Wichita State University for the support and helping me to acquire the technical foundation for my future career. I provide my gratitude to Arun Kaarthick Manoharan for the support and the timely guidance he provided related to my class projects, research, and beyond academia.

Finally, I would like to thank my parents Murali and Vasanthi, my sisters Swetha and Sneha, brother-in-law's Prahadeesh and Vijay Vikram, my most favorite kids Ananyaa and Aditi, my friends Ahilan, Padmapriya, Varsha, Gayatri, Aishwarya, Rajesh, John, Preetha, Anurathi, Naveen, Saravanan, Gratias, Abarnaa, Nimanthi, NaveenKumar, Sherwin, Sudhakar, Fermi, Vijay, Vinoth, Srinivas, Keshav, Thejas, JayaKumar, Ananya, Prajakta, Koushik, Chinmay, Pradeep and my stress busters Ria and Vihaan, for bearing with me and being there for me throughout this journey.

ABSTRACT

The development of new technology and changes in the climatic conditions brought some new methods in the generation of power. Along with these came the advancements of communication and control infrastructure of cyber which along with the traditional power system infrastructure, plays a vital role in delivering power to the customers. The main aim of the utility is to satisfy the customer's need with uninterrupted power supply throughout the year. The power distribution system experiences 70%-80% of power outages due to failure of the component. To reduce the failure in a radial distribution system, it is necessary to evaluate the reliability of the system accurately at the planning stage. This becomes a concern as the traditional power reliability evaluation does not include the cyber equipment induced failures.

In this work a new Boolean algebra based cyber-power interdependency modeling is proposed for reliability evaluation of cyber-enabled power system. This thesis discusses the problems in evaluating the reliability of a cyber power system and different methodologies proposed in the literature. Also, the proposed method is used to evaluate the reliability of Bus 2 of Roy Billinton Test System and obtained results show the significance of cyber-power dependency modeling for system reliability evaluation. Furthermore, the proposed method is compared with an existing technique to show the efficiency in terms of execution time.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

IEEE	Institute of Electrical and Electronics Engineers
LCU	Local Control Unit
FMEA	Failure Mode and Effects Analysis
RBTS	Roy Billinton Test System
ENS	Energy Not Served
SAIDI	System Average Interruption Duration Index
BIBC	Bus Injection to Branch Current
CPIM	Cyber Physical Interdependency Matrix
TSMC	Time Sequential Monte Carlo

CHAPTER 1

INTRODUCTION

Effective utilization of information and control technologies are critical to future grid. The transformation from a traditional power system into a cyber enabled power system calls for changes in the existing system operational procedures, policies, regulations, and standards. As such the modifications to existing system analyses techniques (reliability evaluation), account for the added infrastructure and its impact, are of paramount significance.

1.1 Background and Motivation

In [1], the reliability model for each component is discussed by Amanulla et al. as shown in Figure 1.1, Figure 1.2, Figure 1.3. In Figure 1.1, the component goes from UP state (normal operation) to DOWN state (maintenance, end of life, active failure, and passive failure). During active failure, the component in directly affected and failed. Passive failure occurs when failure of any components in the system indirectly leads to the failure of generator or transformer. They use minimal cut-set method to evaluate the reliability of the system.

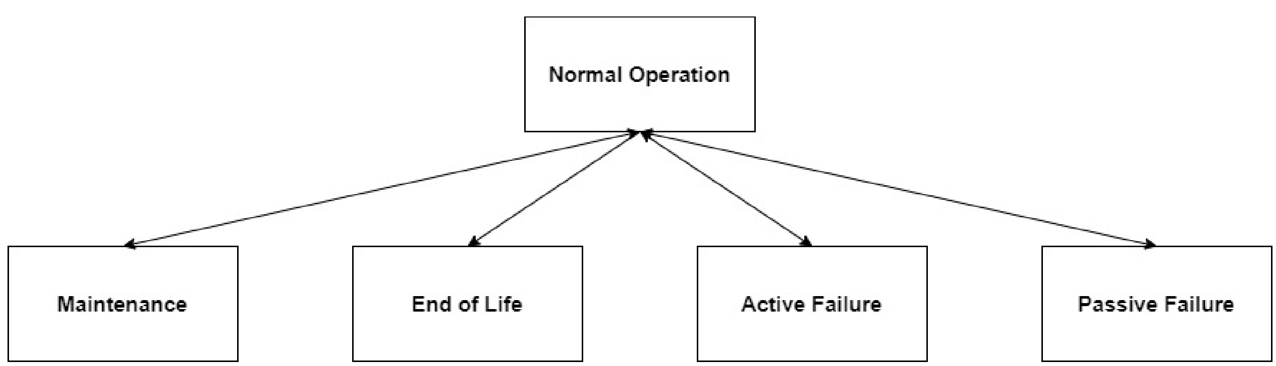

Figure 1.1: Reliability Model for Generator, Transformer and Circuit Breaker

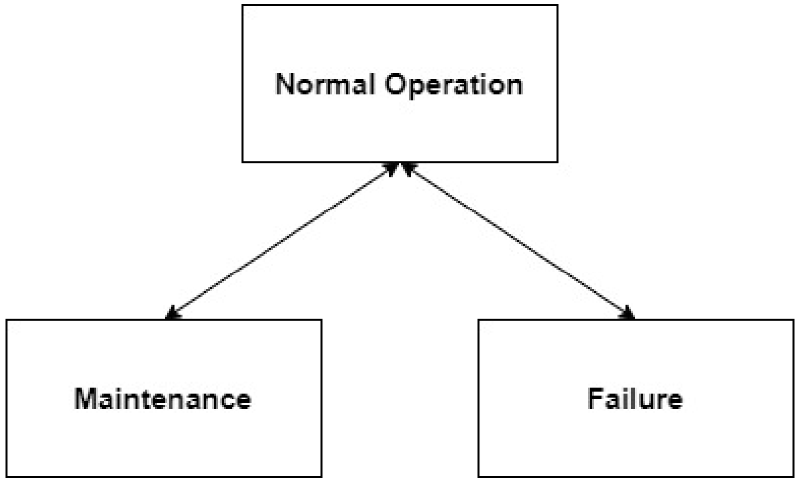

Figure 1.2: Reliability Model for Bus

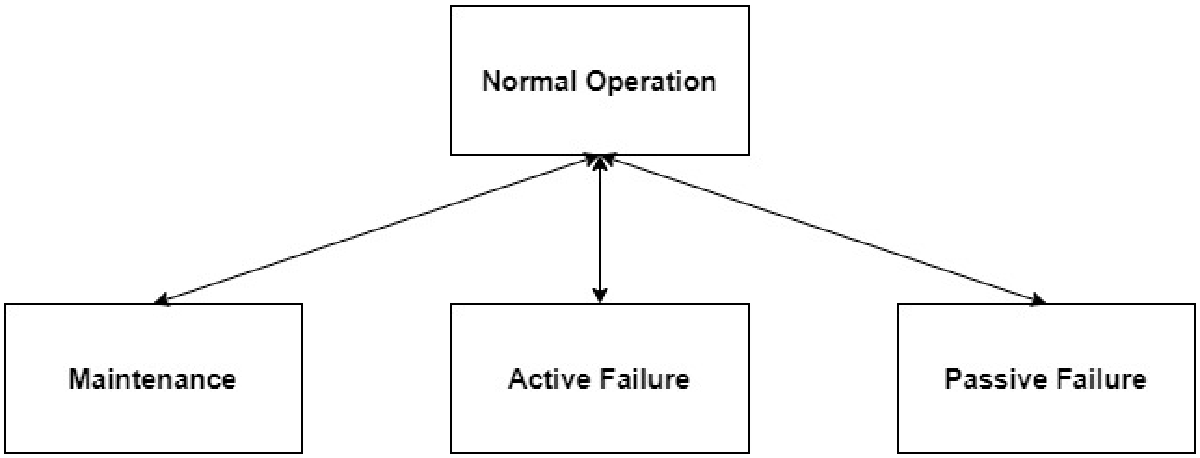

Figure 1.3: Reliability Model for Transmission Line and Switch

As explained before, Figure 1.2 and Figure 1.3 also show how the components (bus, transmission line, and switch) goes from UP state to DOWN state. In [2], Lata et al. discusses about some of the issues of concern in power system reliability and gets into some of the commonly used methods for reliability evaluation as shown in Figure 1.4. The Figure 1.4 shows the most common technique for reliability evaluation which is analytical and simulation. The analytical method is further divided into minimal cut sets and Markov model. The minimal cuts will give the combination of failure of any components which leads to the failure of the system. The simulation-based method is divided into sequential and non-sequential Monte Carlo. In general, sequential Monte Carlo is used to find the reliability of a physical component and for cyber component non-sequential Monte Carlo is used.

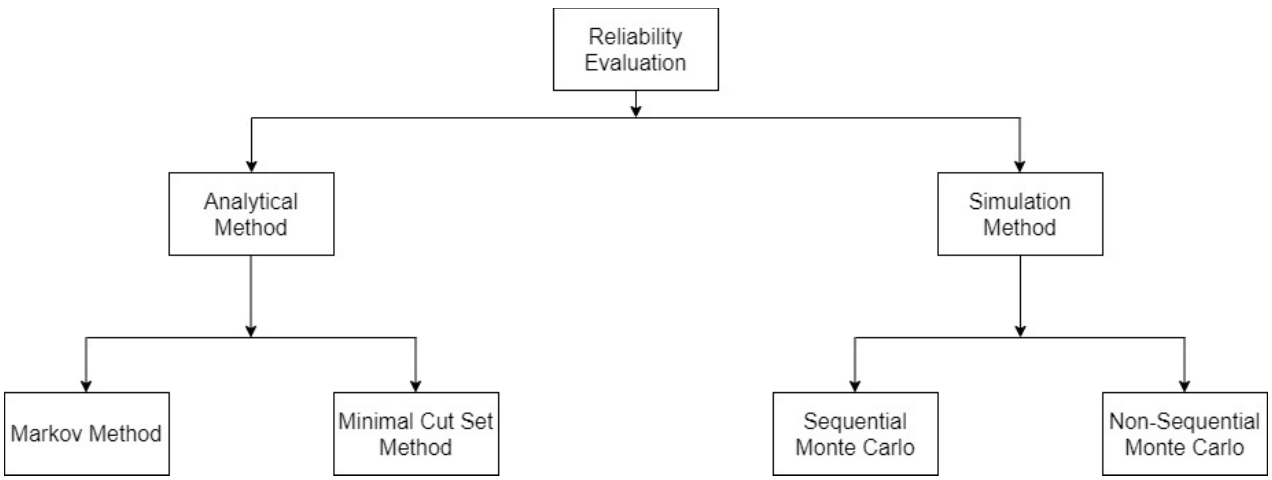

Figure 1.4: Methods of Reliability Evaluation

In [3], Allan et al. discusses about the general data of a RBTS system and provides all data for the reliability evaluation of a distribution system. Billinton et al. [4] compares the reliability indices of utilities from US and Canada. Here, the author measures the past performances of the system and based on that predicts the reliability of a distribution system in future. Jiang et al. [5] proposed a multistate Markov model for the reliability evaluation of the power system, considering the failure of protection devices. The multistate model includes the state which is not faulted and the faulted state before and after switching.

Singh et al. [6] proposed a Markov model for reliability evaluation. They consider all the states in the state space to compute the steady-state system failure probability. Each state is represented by 2-state model of all components in the systems. Considers the minimal cut-sets of the system to compute the steady-state system failure probability. Each minimal cut-set consists of combination of individual component failures which leads to the system failure. Similarly, in [7], the author uses the Markov method. Here, they use DC optimal power flow to find the minimal cut sets.

In [8] Singh et al. generates a sequence of events using random numbers (0/1) based on probability distribution of individual component failures. Sequence generation continues until the change in system reliability between two iterations is less than tolerance. The sequence generation is like exploring the state space, but more realistic for physical system failure studies. The representative state space generated effectively captures the possible failure modes. States are drawn based on the probability distributions of component states and random numbers. States are also drawn separately for each component and the sequence does not follow any chronological order.

In [9], the author uses non-sequential Monte Carlo simulation which is the combination of sequential and random sampling. The representative state space generated from sequential Monte Carlo is randomly sampled for analysis. This is done to overcome time and space complexity of purely sequential Monte Carlo. In [10] Yun et al. proposes a reliability evaluation method for capturing the momentary interruptions. Also, they find the reliability cost estimation for sustained and momentary interruptions. Time sequential Monte Carlo method is used here. In [11], Billinton et al. proposes a time sequential Monte Carlo technique to find the reliability of the system. Here, the type and location of the fault is found, and the load points affected is determined. A random number is generated for the failure of each component and the same procedure is repeated until the desired number of years.

Minimal cut set is one of the most common method for reliability evaluation of power system. Singh et al. [12] proposes a minimal cut set and state space approach for dependent failures in the system which also includes the failure of the standby generators and uninterruptible power supply system. In [13], Behzadirafi et al. proposed a circuit theory-based cut set method for reliability evaluation. As minimal cut set method is one of the common approaches to find the reliability of the system, the authors in [14-19] use different techniques to generate the minimal cut set for the system. In [20], Al-Muhaini et al. proposes a concept of prime number encoding and petri nets to find the minimal cut sets and using Markov model the reliability of the system is evaluated. In [21], Timalsena et al. proposes a nodal analysis approach to find the minimal cut set and evaluate the reliability of the circuit breaker failure in a system.

In the case of power system reliability evaluation, the need for new approaches to include the cyber impact, stems from the following:

Modeling Cyber failure:

(i) Cyber failure does not follow the failure probability distribution as power equipment: This creates a challenge in case of using reliability evaluation through traditional time series Monte Carlo simulation (TSMC). The techniques that use TSMC to represent failure probability with time must be modified to account for the stochastic/intermittent nature of cyber failures.

(ii) Repair/recovery time of cyber failures must be modeled: A cyber failures could result from many reasons ranging from cyber-attack, delay in communication or a glitch in the control software. This calls for detailed modeling of cyber failure modes.

Cyber failure mode and effect analysis:

(iii) Cyber failure is not equal to failure to supply load: Unlike traditional power equipment failure (such as line/transformer failure), cyber failure (such as temperature sensor, fault indication etc.,) may not lead to end customers losing power. But these may aggravate the chance of failure or the failure duration.

(iv) Cyber interdependency modeling: To know the resultant of a cyber failure it is necessary to model the interaction/interdependency

(v) Integrating (i) through (iv) as a part of system failure mode and effect analysis: This is needed to have a comprehensive reliability evaluation tool for the future grid.

This thesis proposes a new method to perform system reliability evaluation that includes (iii) to (v). The novelty of the proposed method is the modular design that can accommodate any cyber model with multiple failure modes and effects.

1.2 Organization of the thesis

This thesis consists of six chapters. Chapter 1 discusses the introduction of the thesis. Cyber power system reliability analysis of a radial distribution system is discussed in Chapter 2. Proposed methodology is presented in Chapter 3. Numerical analysis of case study and validation is done in Chapter 4. Chapter 5 ends the thesis with the conclusion and future work. Finally, the references used are mentioned .

CHAPTER 2

CYBER POWER SYSTEM RELIABILITY

2.1 Prior efforts on modeling cyber impact in reliability analysis

The cyber-physical power system consists of three layers, which are physical, communication and decision [22]. The physical layer consists of the equipment's for generation, transmission, and distribution of power to the customers. The communication layer consists of the sensors for communication and the decision layer decides the operation to be performed during failures. This is shown in Figure 2.1.

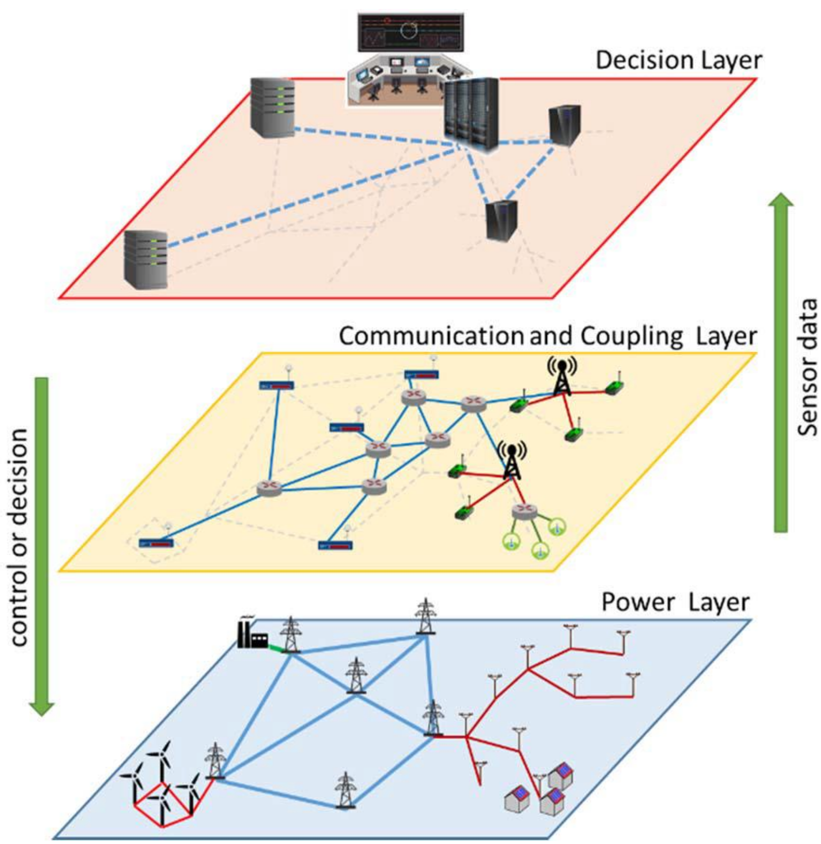

Figure 2.1: Three Layers of Cyber-Physical Power System

As communication entered the traditional power system, the distribution system with the automated switches is controlled from a control center. An LCU (Local Control Unit) is placed at each automated switch and the open/close operation of switches is controlled from a remote-control center which is represented in Figure 2.2.

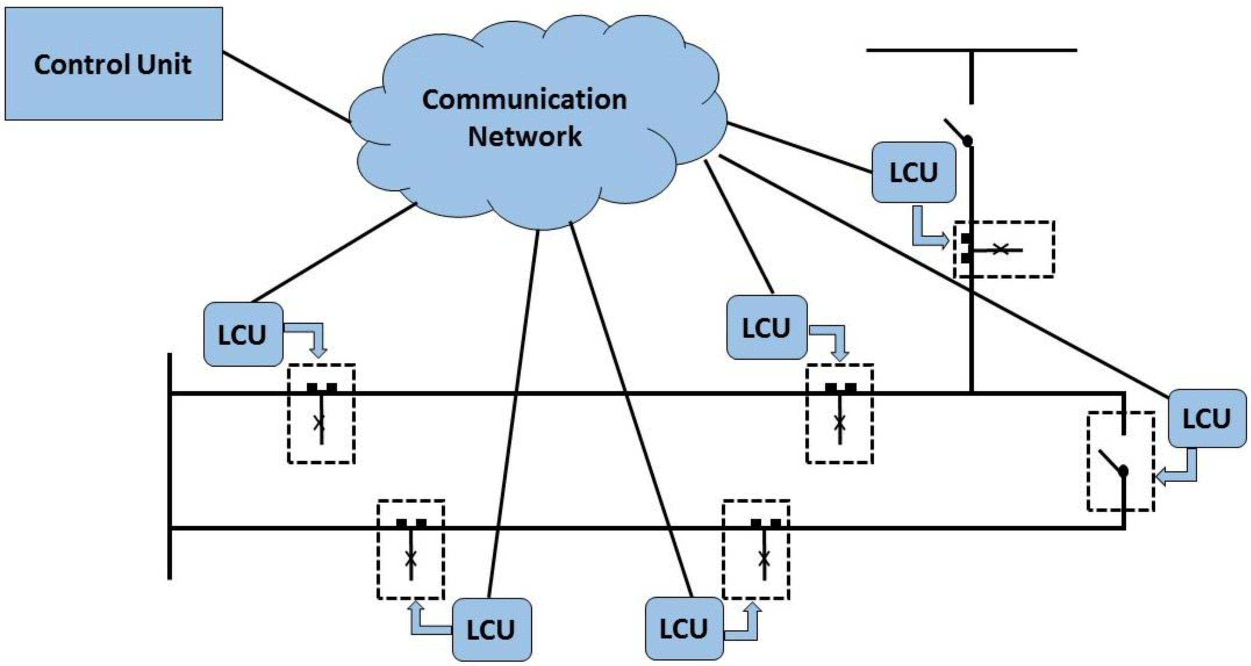

Figure 2.2: Operation of Automated Switches

As more communication devices are added to the distribution system to make our work easy, assessing the reliability of the cyber-physical power system is very important. Different control schemes for the reliability evaluation of power systems are discussed in the literatures.

In [22], Chakraborty et al. proposed a new methodology for the evaluation of reliability of cyber system. Using the concept of three-layered system approach, the reliability of communication and decision layer in a cyber-physical power system is assessed. Aravinthan et al. [23] defines a three-layer model and form a generalized framework for combined (physical and cyber) reliability modeling.

In [24], Lei et al. proposes a benchmark test system for the reliability evaluation of power system when cyber infrastructure is added to it and in [25-27], different available interdependencies in a cyber-physical system are shown. Based on the nature and place of failures in the cyber network, four types of cyber-power interdependencies are categorized as shown in Figure 2.3.

1. Direct Element-Element Interdependencies (DEEI) – Failure of any element in one network will directly impact the element in other network.
2. Direct Network-Element Interdependencies (DNEI) – Performance of one network will directly impact the failure of any element in other network.
3. Indirect Element-Element Interdependencies (IEEI) – Failure of element in a network will not directly impact the element in other network, but indirectly affects the element behavior.
4. Indirect Network-Element Interdependencies (INEI) – Performance of a network will not directly impact the element in another network, but indirectly affects the element behavior.

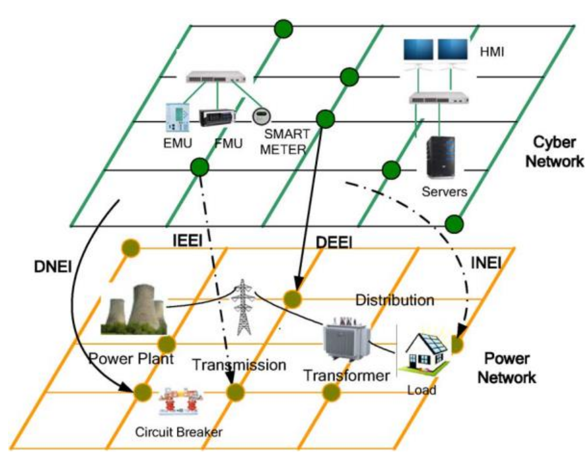

Figure 2.3: Cyber-Physical Interdependencies

In [28-29], Sepehry et al. proposes a BIBC based FMEA (Failure Mode Effect Analysis) method for the reliability evaluation of a radial distribution system. In [30], Heidari-Kapourchali et al. uses the same method used in [28-29] to find the reliability, and in addition added the cyber components to the physical power system. Also, they consider only single component failure at a time and failure of multiple components is not illustrated. They consider any failure occurred in the feeder can be recovered from alternate path supply.

In [31], Lei et al. propose a cyber interdependency matrix to interconnect the physical and cyber system. Here, the interdependency matrix is used to find the failure of the cyber device which leads to the failure of any physical device, from which the cyber-physical power system reliability is evaluated. In [32-33], Liu et al. proposed a method for tracking the direct and indirect interdependencies of cyber component in a cyber-physical system when communication link fails, and the reliability of the system is evaluated using minimal cut-set method. Here, the communication topology which they consider is either star or mesh and not the combination of both (Hybrid).

When the traditional power system devices get upgraded to cyber-power devices, the associated communication topology and protocols must be standardized. In that aspect Ghorbani et al. in [34] proposed a communication network topology for monitoring and self-healing applications in radial distribution system. In [35], Suvagata et al. discuss the impact of communication infrastructure failure on the system reliability in both substation-centered and decentralized multi-agent (FA-Feeder Agent, ZA-Zone Agent, SA-Substation Agent, GA-Generation Agent, and LA-Load Agent) restoration management as shown in Figure 2.4. Each distributed generation is connected to an agent (GA). The Zone Agent in Multi-agent system structure is responsible for coordination and management of generation agent (GA) and load agent (LA). Each Zone agent (ZA) sends all the required information's to the respective Feeder agent (FA). Substation agent is installed at substation level and manages substation equipment and receives feeder level information. Also, they discuss about the cyber-physical interdependencies of components based on their functionality.

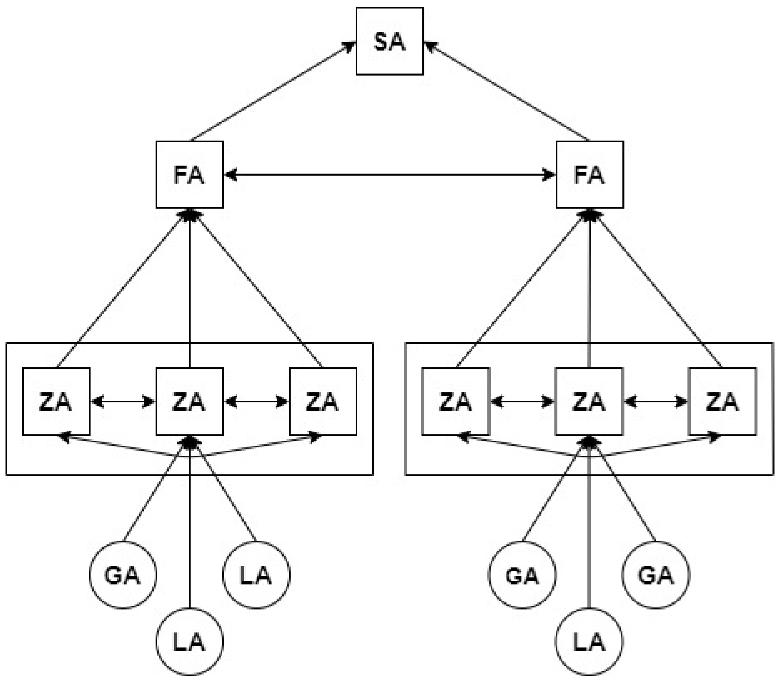

Figure 2.4: Multi-Agent Layout of a Power Distribution System

2.2 Research Gap

All the above-mentioned work forms the base for this thesis. The novelty of this work is incorporating physical layer, communication layer and decision layer in a single radial distribution network and analyzing the reliability of the cyber-physical system. In the proposed method the reliability analysis of cyber-physical interdependencies is tracked based on the functionality of the component. And the proposed method tracks the failure of multiple components using Boolean logic and the communication system in the proposed system will work in star, mesh, and hybrid topology. Chapter 3 will explain the Proposed method for this reliability analysis.

CHAPTER 3

PROPOSED METHOD

The novelty of the proposed method is the use of Boolean arithmetic operations to capture the failure effect of multiple component failure modes. In addition, the proposed algorithm also accounts for the load point outage restoration using alternate path of power supply. This can be explained using the following fictitious system. Consider a system with three load points (1, 2 & 3) and three components (A, B & C). For this system, the failure effect of individual component on load point outage in normal and alternate path is given by Table 3.1 and 3.2, respectively. Here, 1 represents load point outage for the corresponding component outage and 0 represents no impact on the load point for the corresponding component outage.

Table 3.1: Normal Path

Component	Load Point 1	Load Point 2	Load Point 3
A	1	1	0
B	0	1	1
C	1	1	1

Table 3.2: Alternate Path

Component	Load Point 1	Load Point 2	Load Point 3
A	1	0	0
B	0	1	0
C	1	1	1

Let us consider the failure effect of combined failure of components A & B. To evaluate the load point outage resulting from this scenario, the proposed method implements the following procedure,

- Element wise OR operations of arrays corresponding to the rows of component A & B in normal path table.
- Element wise OR operations of arrays corresponding to the rows of component A & B in alternate path table.
- Element wise AND operation of arrays resulting in step 1 and 2 respectively. This resultant array will give us the impact of considered component failure on load point outage.

If we follow the above procedure for scenario of component A & B failing, it will resemble the following.

$$Component\ A_{normal\ path} \oplus Component\ B_{normal\ path} = R_1 = [1 \quad 1 \quad 1]$$

$$Component\ A_{alternate\ path} \oplus Component\ B_{alternate\ path} = R_2 = [1 \quad 1 \quad 0]$$

$$R_1 \otimes R_2 = [1 \quad 1 \quad 0]$$

3.1 Demonstration with a simple radial network

A simple equivalent radial distribution network is used for this thesis. The main aim of this work is to analyze the reliability of a cyber-physical power system and compare the results when the systems communication and decision is 100% reliable. To perform this analysis, a radial distribution network is considered as shown in the Figure 3.1, and the following procedure is used to perform the analysis.

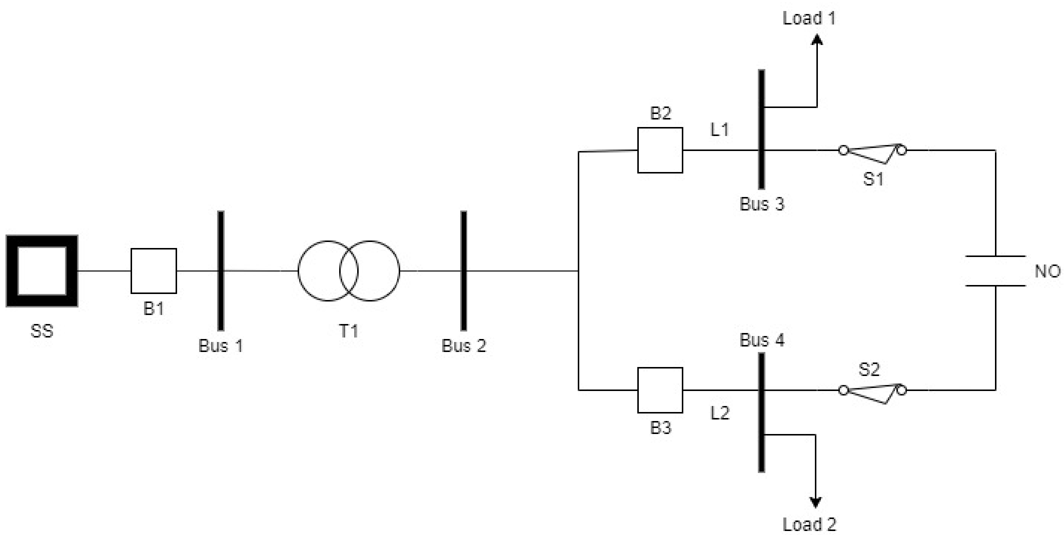

Figure 3.1: Radial Distribution Network

Let us consider this simple radial distribution network for reliability analysis of a cyber-physical system. Here,

SS – Substation

B – Breaker

L – Line

S – Disconnect Switch

T – Transformer

NO – Normally Open Switch

In the proposed method, firstly a connection matrix for the radial distribution system is framed with both normal path and alternate path of supply which also includes the communication devices. A matrix for line protection devices is also developed.

Table 3.3: Connection Matrix for Normal Path

Component / Load Point	Load Point 1	Load Point 2
B1 – H	1	1
B1 – C	1	1
B2 – H	1	0
B2 – C	1	1
B3 – H	0	1
B3 – C	1	1
T1	1	1
S1 – H	0	0
S1 – C	1	0
S2 – H	0	0
S2 – C	0	1
L1	1	0
L2	0	1
NO	0	0

Where,

H – Hardware

C – Cyber

1 – Not Working

0 – Working

Table 3.3. represents the connection matrix of the radial distribution network using the supply through normal path. Here, each load point gets the power supply from the substation using normal path. The 1's in the above table represents the failure of each components and the effect it has on each load point. For e.g., if the hardware of breaker 1 fails, it causes outage in both the load points. At the same time if line 1 fails, it causes outage at load point 1 and load point 2 still gets the supply. Similar way Table 3.3 deals with failure of all the components present in the distribution network shown in Figure 3.3, and its effect on each load point.

Table 3.4: Connection Matrix for Load Point Failure in Alternate Path

Component / Load Point	Load Point 1	Load Point 2
B1 – H	1	1
B1 – C	1	1
B2 – H	0	1
B2 – C	1	1
B3 – H	1	0
B3 – C	1	1
T1	1	1
S1 – H	1	1
S1 – C	1	1
S2 – H	1	1
S2 – C	1	1
L1	1	1
L2	1	1
NO	1	1

Where,

H – Hardware

C – Cyber

1 – Not Working

0 – Working

Table 3.4. represents the connection matrix of the radial distribution network using the supply through alternate path. Here, each load point gets the power supply from the substation using alternate path. The 1's in the above table represents the failure of which components affects the supply to the load through alternate path. For e.g., if the hardware of breaker 2 fails, it causes outage only at load point 2 and load point 1 still gets the supply by alternate path. At the same time if line 1 fails, it causes outage at both the load points. Similar way Table 3.4 deals with failure

of all the components present in the distribution network shown in Figure 3.1, which affect the alternate path of supply and its effect on each load point.

Table 3.5: Line Protection Devices Matrix

Line / Protection Devices	B1	B2	B3
L1	0	1	0
L2	0	0	1

Where,

1 – Not Working

0 – Working

Table 3.5. represents the protection devices respected to each line. Here, we will come to know about the protection devices related to each line which are represented using 1's. For e.g., B2 is protection devices for line L1, so it is represented by 1 and the other protection devices B1, B3 are represented by 0.

Secondly, once the line protection device matrix and connection matrix for normal path and alternate path is formed, then the main analysis of reliability starts. The step-by-step procedure for reliability analysis of a cyber-physical system is given below,

- First step is to find the components which are failed in the system.
- Next check whether line failure occurred in the system.
- If line failure occurred, then go to Table 3.3, and check for the failure of protection devices of that line.
- If any of that line protection device fails, check.

$$L\left(\overline{S^H} * \left(S^C + \left(S^D * \overline{S^C}\right)\right)\right) == 1 \tag{3.1}$$

$$L\left(\overline{B^H} * \left(B^C + \left(B^D * \overline{B^C}\right)\right)\right) == 1 \tag{3.2}$$

Where,

L – Line

S^H- Switch Hardware

S^C- Switch Communication

S^D- Switch Decision

B^H- Breaker Hardware

B^C- Breaker Communication

B^D- Breaker Decision

- If equation (3.1) or (3.2) are equal to 1, it is considered as communication device of that component has failed and determine the load point outage.

$$Load\ Point\ Outage = \ (OR\ of\ failure\ effects\ of\ communication\ devices\ in\ normal\ path\ )\ AND\ (OR\ of\ failures\ effectes\ of\ communication\ devices\ in\ alternate\ path\ )$$

- If equation (3.1) or (3.2) are equal to 0, it is considered as communication device of that component is working and the device hardware has failed, and load point outage is determined.

$$Load\ Point\ Outage = \ (OR\ of\ failure\ effects\ in\ normal\ path\ )\ AND\ (OR\ of\ failures\ effectes\ in\ alternate\ path\ )$$

- Failures which are not recovered using alternate path: To find the load point failures which are not recovered, outage not recovered is determined.

$$Outage\ Not\ Recovered = (Load\ Point\ Outage)\ AND\ (OR\ of\ failure\ effects\ in\ normal\ path)$$

- Failures which are recovered using alternate path: To find the load point failures which are recovered, Outage Recovered is determined.

$$Outage\ Recovered = \left(\overline{Load\ Point\ Outage}\right)\ AND\ (OR\ of\ failures\ effects\ in\ normal\ path)$$

- Total number of interruptions occurred in the system.

$$Total\ Interruptions = Outage\ Not\ Recovered + Outage\ Recovered$$

- Next step is to find the Total outage time.

$$Total\ Outage\ Time = (Outage\ Not\ Recovered * Repair\ Time) + (Outage\ Recovered * Repair\ Time)$$

- Now find the reliability indices SAIDI and ENS

$$SAIDI = \frac{Total\ Outage\ Time}{Total\ Customers}$$

$$ENS = Total\ Outage\ Time * Total\ Power\ Supplied$$

Finally, the outage occurred at each load point due to the failure in any of the components in the radial distribution network is found from the procedure discussed above. SAIDI and ENS can be found based on the repair time, switching time and total number of customers at each load point, once the outage at each load point is found. Thus, the reliability evaluation of a cyber-physical system is discussed in the proposed method. The proposed method can be used for any complex network by making changes in Table 3.3, Table 3.4 and Table 3.5 based on the given radial distribution network. The proposed control scheme is shown in Figure 3.2. The proposed method is implemented in the Bus 2 of Roy Billinton Test System (RBTS) with variations in the reliability of the cyber-component (Communication and Decision) in steps and compared to an existing method in the next chapter.

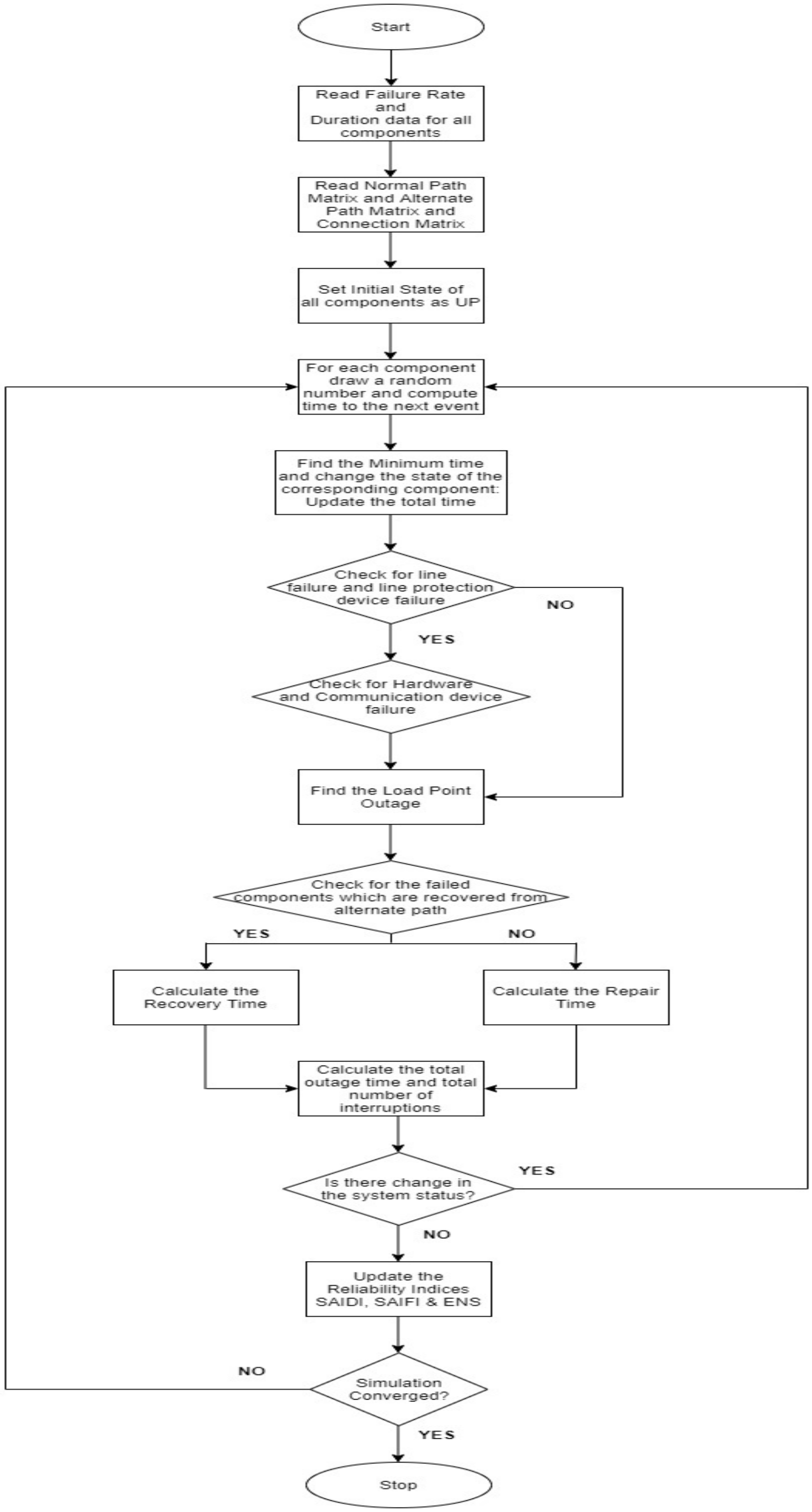

Figure 3.2: Proposed Control Scheme

CHAPTER 4

NUMERICAL ANALYSIS OF CASE STUDY AND VALIDATION

4.1 Comparison with the existing method

The proposed method is implemented in a Modified RBTS (Bus-2) shown in figure 4.1 and the results are compared with one of the methods proposed by Sepehry et al. in [30].

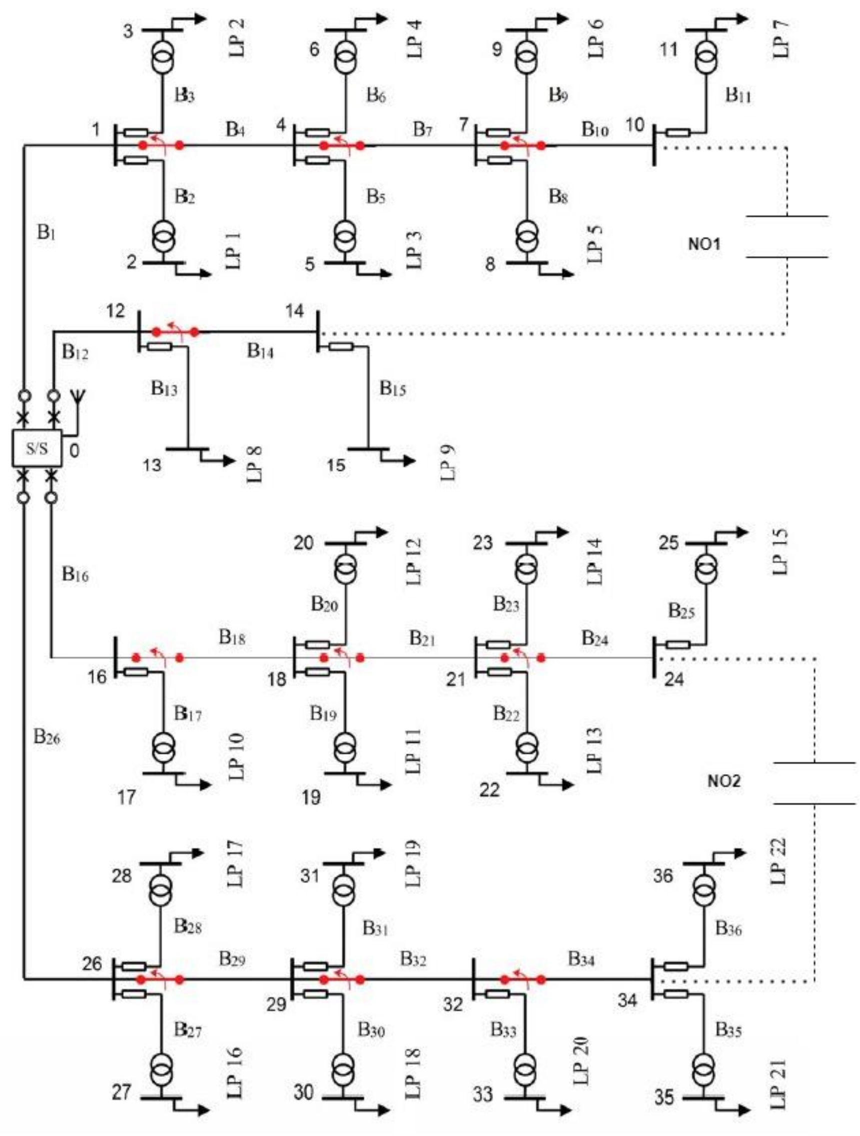

Fig 4.1: Modified RBTS Bus – 2

To show the application of the proposed method with a smaller number of protection devices, some modifications are made to the system. In [30], the authors consider only the active failure, and they assume only one component failure at a time. Multiple component failure is neglected. Also, the author considers all the failure occurred in the feeder can be recovered from the alternate path supply. In [30], the author assumes all the disconnect switches are 100% reliable and they consider only line failure in the system. All other components failures are not considered. During this comparison all the assumptions and system data are taken as same as the author in [30] which is mentioned in Table 4.1.

Table 4.1: Failure Rates and Repair Time of Components

Components/ Failure Rate and Repair Time	Failure Rate (Failures/Year/km)	Repair Time (Hours)
Line	0.0650	5
Disconnect Switch	0	1

The failure rate of communication is varied in three steps {0, 0.05, 0.1} and the repair time is assumed to be 2.5 hours. The proposed method also considers the same assumption and the ENS obtained is compared with [30]. The results obtained are almost similar with a difference of less than 0.5% and the proposed method reduces the runtime by 36% which is mentioned in Table 4.2 and Table 4.3. Also, the comparison between the two methods is plotted in fig.4.2 and fig.4.3.

Table 4.2: ENS Comparison Results

Cases	BIBC Based FMEA Method ENS ((kWh/Year) (Hours)	Proposed Method ENS (kWh/Year)
100 % Communication	65.101	65.073
95 % Communication	65.257	65.083
90 % Communication	65.415	65.105

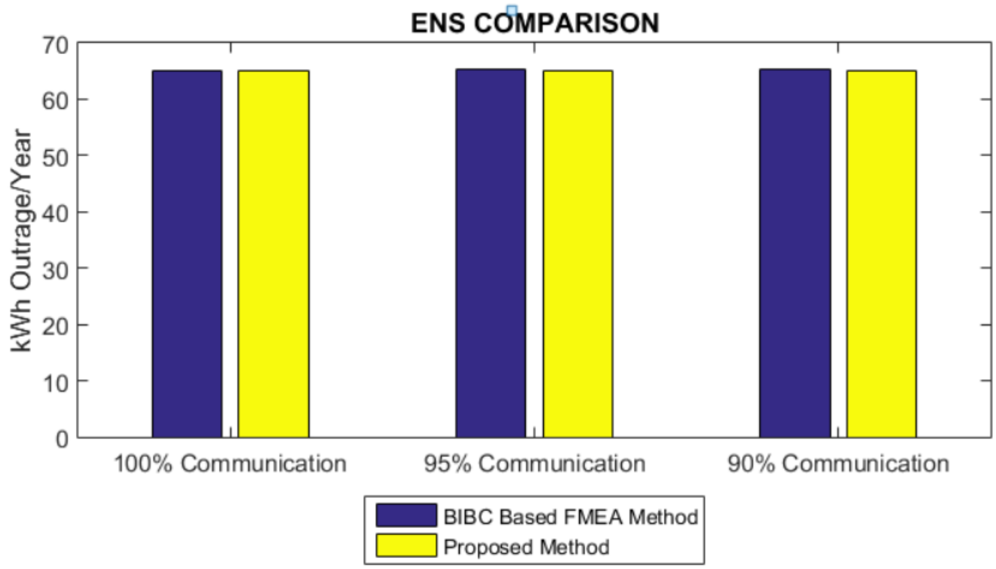

Fig.4.2: ENS Comparison

Table 4.3: Runtime Comparison Results

BIBC Based FMEA Method Average Runtime (Seconds)	**Proposed Method Average Runtime (Seconds)**
13.579	8.771

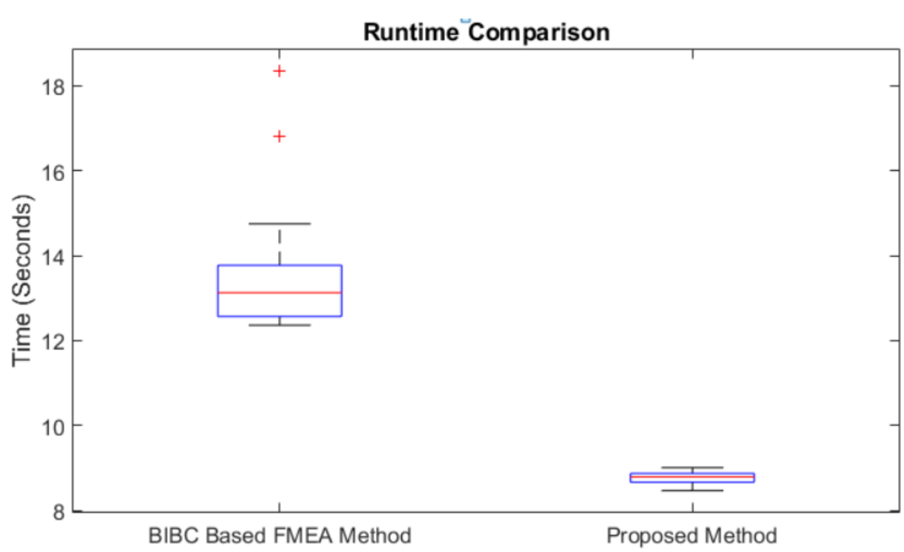

Fig.4.3: Runtime comparison

4.2 Case study with communication and decision failures

The Proposed method is applied to the bus 2 of the RBTS system, considering communication and decision failure. To show the application of the proposed method with a smaller number of protection devices, some modifications are made to the system as shown in figure 4.1. The proposed system considers all the components in the test system and the system data are taken from [36]. Here, disconnects switch and circuit breaker are assumed to have cyber components. Both the communication and decision failures are varied in three steps {0, 0.05, 0.1} and the reliability indices (SAIDI and ENS) are calculated.

Table 4.4: Failure Rate and Repair Time of Components

Components / Failure Rate and Repair Time	Failure Rate (Failures/Year/km)	Repair Time (Hours)
Transformer	0.0150	10
Breaker	0.0040	4
Disconnect Switch	0.0040	4
Line	0.0650	2
Fuse	0.0001	1
Bus	0.0010	2

The failure rate and repair time which are considered for this reliability evaluation is mentioned in Table 4.4 and the results are shown in Table 4.5. In Table 4.5, the reliability Indices are evaluated for 9 different combination of communication and decision failures. Here, we can notice as the failure rate of communication and decision increases, the SAIDI and ENS increases. All the results are plotted in figure 4.4 and figure 4.5 and the trend shows that the cumulative failure of communication and decision has same impact in SAIDI and ENS. This is because the repair time of communication and decision is assumed to be same.

Table 4.5: Results of SAIDI and ENS

Case	Communication Failure (Failures/Year)	Decision Failure (Failures/Year)	SAIDI (Duration of Interruptions in Hours/Year/Customer)	ENS (kWh Outage/Year)
1	0	0	3.6117	62.0612
2	0	0.05	6.8688	127.6834
3	0	0.1	10.1247	193.2941
4	0.05	0	6.8694	127.6807
5	0.05	0.05	10.1216	193.2622
6	0.05	0.1	13.3776	258.8398
7	0.1	0	10.1256	193.3041
8	0.1	0.05	13.3764	258.8263
9	0.1	0.1	16.6314	324.4109

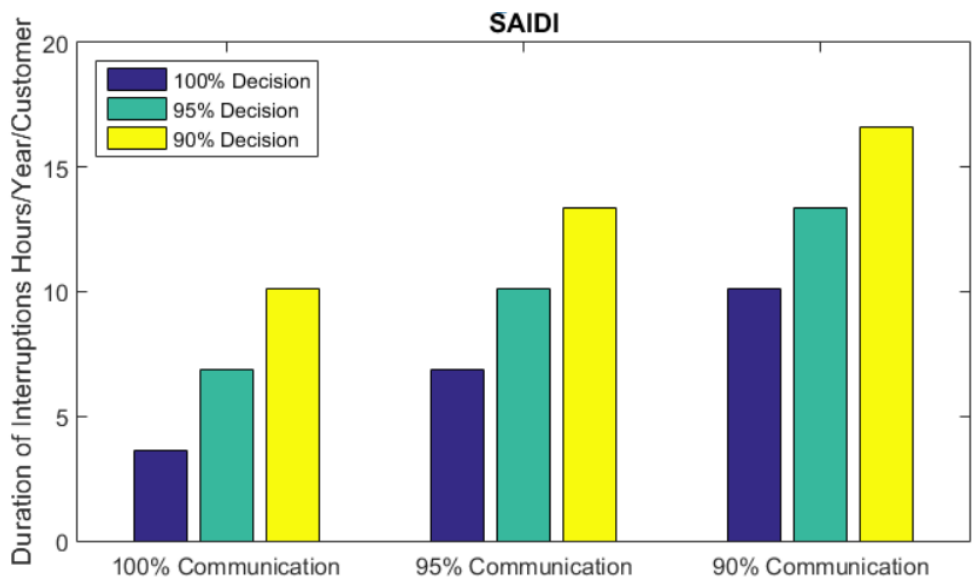

Fig.4.4: Results of SAIDI

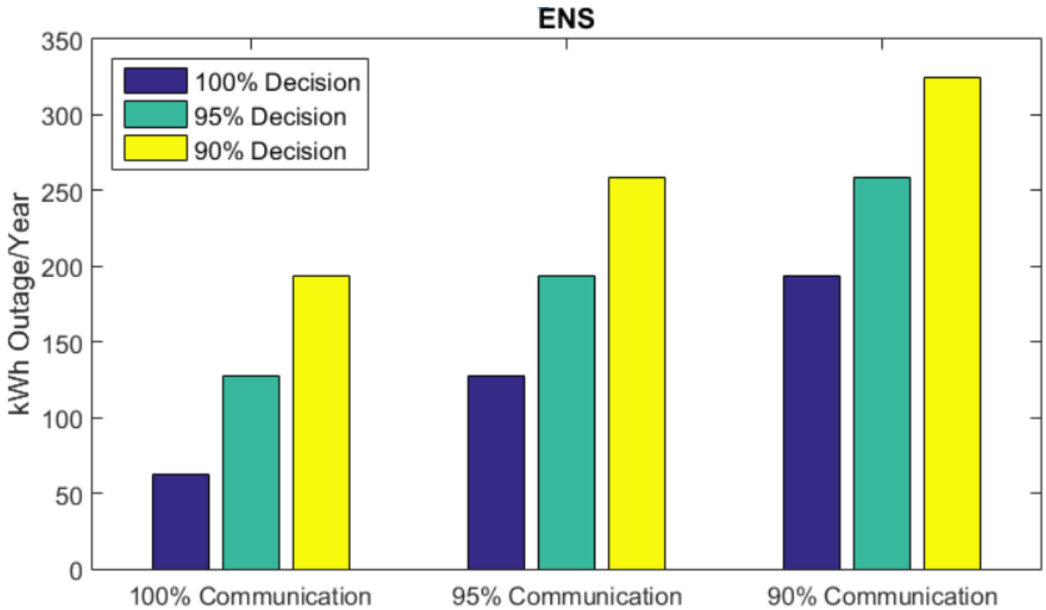

Figure 4.5: Results of ENS

CHAPTER 5

CONCLUSION AND FUTURE WORK

As the cyber devices added to the system, it is necessary to find the reliability of the system including those cyber devices. This thesis discusses the reliability analysis of a cyber-physical system, which includes communication and decision failures. The novelty of the proposed method is the modular design of the reliability evaluation process that can integrate the communication and decision topology and the corresponding failure modes and effects.

The numerical analysis presented show the variations in the reliability of the system when the communication and decision is considered as 100% reliable and considering their unavailability. In addition, the proposed method was also validated against an existing method and it was seen that the proposed method provided similar results with about 36% reduction in execution time. These signify the effectiveness of the proposed method for the reliability evaluation of cyber enabled radial distribution system with alternate supply paths through reconfiguration.

As the technology has improved, the cyber-attacks made using those technology has also increased. Hence modeling the impact of cyber-attacks to the power system will make our system more reliable and secure.

REFERENCES

REFERENCES

[1] B. Amanulla, S. Chakrabarti and S. N. Singh, "Reconfiguration of Power Distribution Systems Considering Reliability and Power Loss," in IEEE Transactions on Power Delivery, vol. 27, no. 2, pp. 918-926, April 2012, doi: 10.1109/TPWRD.2011.2179950.

[2] P. Lata and S. Vadhera, "Issues of concerns in power system reliability," 2015 International Conference on Power, Instrumentation, Control and Computing (PICC), Thrissur, 2015, pp. 1-6, doi: 10.1109/PICC.2015.7455772.

[3] R. N. Allan, R. Billinton, I. Sjarief, L. Goel and K. S. So, "A reliability test system for educational purposes-basic distribution system data and results," in IEEE Transactions on Power Systems, vol. 6, no. 2, pp. 813-820, May 1991, doi: 10.1109/59.76730.

[4] R. Billinton and J. Billinton, "Distribution system reliability indices," in IEEE Transactions on Power Delivery, vol. 4, no. 1, pp. 561-568, Jan. 1989, doi: 10.1109/61.19247.

[5] K. Jiang and C. Singh, "New Models and Concepts for Power System Reliability Evaluation Including Protection System Failures," in IEEE Transactions on Power Systems, vol. 26, no. 4, pp. 1845-1855, Nov. 2011, doi: 10.1109/TPWRS.2011.2156820.

[6] Singh, Chanan, and Roy Billinton. *System reliability, modelling and evaluation*. Vol. 769. London: Hutchinson, 1977.

[7] Y. Liu and C. Singh, "Reliability Evaluation of Composite Power Systems Using Markov Cut-Set Method," in IEEE Transactions on Power Systems, vol. 25, no. 2, pp. 777-785, May 2010, doi: 10.1109/TPWRS.2009.2033802.

[8] C. Singh and J. Mitra, "Monte Carlo simulation for reliability analysis of emergency and standby power systems," IAS '95. Conference Record of the 1995 IEEE Industry Applications Conference Thirtieth IAS Annual Meeting, Orlando, FL, USA, 1995, pp. 2290-2295 vol.3, doi: 10.1109/IAS.1995.530594.

[9] H. Lei and C. Singh, "Non-Sequential Monte Carlo Simulation for Cyber-Induced Dependent Failures in Composite Power System Reliability Evaluation," in IEEE Transactions on Power Systems, vol. 32, no. 2, pp. 1064-1072, March 2017, doi: 10.1109/TPWRS.2016.2572159.

[10] S. -. Yun, J. -. Kim, J. -. Moon, C. -. Park, S. -. Park and M. -. Lee, "Reliability evaluation of radial distribution system considering momentary interruptions," 2003 IEEE Power Engineering Society General Meeting (IEEE Cat. No.03CH37491), Toronto, Ont., 2003, pp. 480-485 Vol. 1, doi: 10.1109/PES.2003.1267224.

[11] R. Billinton and Peng Wang, "Teaching distribution system reliability evaluation using Monte Carlo simulation," in IEEE Transactions on Power Systems, vol. 14, no. 2, pp. 397-403, May 1999, doi: 10.1109/59.761856.

[12] C. Singh and N. V. Gubbala, "Reliability analysis of electric supply including standby generators and uninterruptible power supply system," Conference Record of the 1993 IEEE Industry Applications Conference Twenty-Eighth IAS Annual Meeting, Toronto, Ontario, Canada, 1993, pp. 1454-1460 vol.2, doi: 10.1109/IAS.1993.299188.

[13] S. Behzadirafi, H. Salehfar, A. Manoharan, S. R. Nadipalli and V. Aravinthan, "Electric Circuit Theory Based Minimal Cut-Set Realization for Reliability Evaluation of Non-Directional Networks," 2018 North American Power Symposium (NAPS), Fargo, ND, 2018, pp. 1-6, doi: 10.1109/NAPS.2018.8600575.

[14] Z. Miao, R. Niu, T. Tang and J. Liu, "A new generation algorithm of fault tree minimal cut sets and its application in CBTC system," 2013 IEEE International Conference on Intelligent Rail Transportation Proceedings, Beijing, 2013, pp. 221-226, doi: 10.1109/ICIRT.2013.6696297.

[15] I. Helal, "A Heuristic-Based Approach for Enumerating The Minimal Path Sets in a Distribution Network," 2007 IEEE Power Engineering Society General Meeting, Tampa, FL, 2007, pp. 1-5, doi: 10.1109/PES.2007.385987.

[16] M. Fotuhi-Firuzabad, R. Billinton, T. S. Munian and B. Vinayagam, "A novel approach to determine minimal tie-sets of complex network," in IEEE Transactions on Reliability, vol. 53, no. 1, pp. 61-70, March 2004, doi: 10.1109/TR.2004.824834.

[17] R. N. Allan, R. Billinton and M. F. De Oliveira, "An Efficient Algorithm for Deducing the Minimal Cuts and Reliability Indices of a General Network Configuration," in IEEE Transactions on Reliability, vol. R-25, no. 4, pp. 226-233, Oct. 1976, doi: 10.1109/TR.1976.5219977.

[18] M. Kvassay and J. Kostolny, "Minimal Cut Sets and Path Sets in Binary Decision Diagrams and logical differential calculus," The 10th International Conference on Digital Technologies 2014, Zilina, 2014, pp. 179-186, doi: 10.1109/DT.2014.6868712.

[19] M. Fotuhi-Firuzabad, R. Billinton, T. S. Munian and B. Vinayagam, "A novel approach to determine minimal tie-sets of complex network," in IEEE Transactions on Reliability, vol. 53, no. 1, pp. 61-70, March 2004, doi: 10.1109/TR.2004.824834.

[20] M. Al-Muhaini and G. T. Heydt, "A Novel Method for Evaluating Future Power Distribution System Reliability," in IEEE Transactions on Power Systems, vol. 28, no. 3, pp. 3018-3027, Aug. 2013, doi: 10.1109/TPWRS.2012.2230195.

[21] K. R. Timalsena, P. Piya and R. Karki, "A Novel Methodology to Incorporate Circuit Breaker Active Failure in Reliability Evaluation of Electrical Distribution Networks," in IEEE Transactions on Power Systems, doi: 10.1109/TPWRS.2020.3010529.

[22] S. Chakraborty, A. Manoharan, A. Hettiarachchige-Don, V. Aravinthan and M. H. Kapourchali, "Model for Evaluating the Reliability of Cyber Component in Power Distribution Systems," *2019 North American Power Symposium (NAPS)*, Wichita, KS, USA, 2019, pp. 1-6.

[23] V. Aravinthan et al., "Reliability Modeling Considerations for Emerging Cyber-Physical Power Systems," *2018 IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)*, Boise, ID, 2018, pp. 1-7.

[24] H. Lei and C. Singh, "Developing a benchmark test system for electric power grid cyber-physical reliability studies," 2016 International Conference on Probabilistic Methods Applied to Power Systems (PMAPS), Beijing, 2016, pp. 1-5, doi: 10.1109/PMAPS.2016.7764053.

[25] B. Falahati and Yong Fu, "A study on interdependencies of cyber-power networks in smart grid applications," 2012 IEEE PES Innovative Smart Grid Technologies (ISGT), Washington, DC, 2012, pp. 1-8, doi: 10.1109/ISGT.2012.6175593.

[26] B. Falahati, Y. Fu and L. Wu, "Reliability Assessment of Smart Grid Considering Direct Cyber-Power Interdependencies," in IEEE Transactions on Smart Grid, vol. 3, no. 3, pp. 1515-1524, Sept. 2012, doi: 10.1109/TSG.2012.2194520.

[27] B. Falahati and Y. Fu, "Reliability Assessment of Smart Grids Considering Indirect Cyber-Power Interdependencies," in IEEE Transactions on Smart Grid, vol. 5, no. 4, pp. 1677-1685, July 2014, doi: 10.1109/TSG.2014.2310742.

[28] M. Sepehry, M. Heidari-Kapourchali, M. R. U. Rahman and V. Aravinthan, "A New Algorithm for Reliability Assessment of Distribution System Based on Reliability Network Equivalent Technique," 2018 IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS), Boise, ID, 2018, pp. 1-5, doi: 10.1109/PMAPS.2018.8440226.

[29] M. Sepehry, M. Heidari-Kapourchali, A. Banajiger and V. Aravinthan, "A new algorithm for reliability evaluation of radial distribution networks," 2014 North American Power Symposium (NAPS), Pullman, WA, 2014, pp. 1-6, doi: 10.1109/NAPS.2014.6965483.

[30] M. Heidari-Kapourchali, M. Sepehry, Long Zhao and V. Aravinthan, "Reliability analysis of cyber-enabled power distribution system using sequential Monte-Carlo," 2015 North American Power Symposium (NAPS), Charlotte, NC, 2015, pp. 1-6, doi: 10.1109/NAPS.2015.7335238.

[31] H. Lei, C. Singh and A. Sprintson, "Reliability Modeling and Analysis of IEC 61850 Based Substation Protection Systems," in IEEE Transactions on Smart Grid, vol. 5, no. 5, pp. 2194-2202, Sept. 2014, doi: 10.1109/TSG.2014.2314616.

[32] W. Liu, Z. Lin, L. Wang, Z. Wang, H. Wang and Q. Gong, "Analytical Reliability Evaluation of Active Distribution Systems Considering Information Link Failures," in IEEE Transactions on Power Systems, vol. 35, no. 6, pp. 4167-4179, Nov. 2020, doi: 10.1109/TPWRS.2020.2995180.

[33] W. Liu, Q. Gong, H. Han, Z. Wang and L. Wang, "Reliability Modeling and Evaluation of Active Cyber Physical Distribution System," in IEEE Transactions on Power Systems, vol. 33, no. 6, pp. 7096-7108, Nov. 2018, doi: 10.1109/TPWRS.2018.2854642.

[34] J. Ghorbani, Y. P. Fallah, M. A. Choudhry and A. Feliachi, "Investigation of communication media requirements for self-healing power distribution systems," 2013 IEEE Energytech, Cleveland, OH, USA, 2013, pp. 1-7, doi: 10.1109/EnergyTech.2013.6645325.

[35] S. Chakraborty, T. Balachandran and V. Aravinthan, "Worst-case reliability modeling and evaluation in cyber-enabled power distribution systems," 2017 North American Power Symposium (NAPS), Morgantown, WV, 2017, pp. 1-6, doi: 10.1109/NAPS.2017.8107279.

[36] Historical Reliability Data for IEEE 3006 Standards: Power Systems Reliability," in *3006HistoricalData-2012 Historical Reliability Data for IEEE 3006 Standards*, vol., no., pp.1-303, 9 Nov. 2012.